AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1-16. (Cancelled)

17. (Previously Presented) Data exchange method between two devices locally connected to one another, a first device of the two devices being a security module and a second device of the two devices being a receiver, the first device comprising at least one first encrypting key of a pair of asymmetric keys and the second device comprising at least the second encrypting key of said pair of asymmetric keys, this method comprising:

- generating, at least one first random number in the first device,
- generating, at least one second random number in the second device,
- encrypting said first random number by said first encrypting key, the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment,
- encrypting said second random number by said second encrypting key, the second encrypting key initialized in the second device during an initialization phase of the second device in a second protected environment,
- transmitting said first encrypted random number to the second device,
- transmitting said second encrypted random number to the first device,
- decrypting the first encrypted random number in said second device,
- decrypting the second encrypted random number in said first device,

- combining said random numbers generated by one of the devices and received by the other device to generate a session key,
- and using the session key to encrypt and decrypt all or part of the exchanged data between the first and second device.

18. (Currently Amended) Data exchange method according to claim 17, wherein the first encrypted random number, transmitted to the second device and decrypted by the second device is~~generated by the first device and decrypted by the second device~~

- ~~is~~ encrypted by said second device by means of said second encrypting key,
- ~~is~~ transmitted in [[a]]an encrypted form to said first device,
- ~~is~~ decrypted in the first device by means of the first encrypting key and
- ~~is~~ compared to said first random number previously generated by the first device, and

wherein [[the]]a data transfer between the first and second devices is stopped if the compared random numbers are not identical.

19. (Currently Amended) Data exchange method according to claim 17, wherein the second random number, transmitted to the first device and decrypted in the first device is~~generated by the second device and decrypted by the first device~~

- ~~is~~ encrypted by said first device by means of said first encrypting key,
- ~~is~~ transmitted in [[a]]an encrypted form to said second device,
- ~~is~~ decrypted in the second device by means of the second encrypting key and
- ~~is~~ compared to said second random number previously generated by the second device, and

wherein [[the]]a data transfer between the first and second devices is stopped if the compared random numbers are not identical.

20. (Previously Presented) Data exchange method according to claim 17, in which said first device and said second device contain a symmetric encrypting key, wherein the random numbers are combined with said symmetric key to generate the session key.

21. (Previously Presented) Data exchange method according to claim 17, wherein the combination of said random numbers is a concatenation.

22. (Previously Presented) Data exchange method according to claim 20, wherein the combination of said random numbers is a concatenation.

23. (Previously Presented) Data exchange method according to claim 17, wherein the session key is regenerated in function of a determined parameter of use.

24. (Previously Presented) Data exchange method according to claim 23, wherein the determined parameter of use is the duration of use.

25. (Previously Presented) Data exchange method according to claim 17, wherein at least one of the two devices measures at least one representative physical parameter of the communication, such as the line impedance and/or the electric consumption, wherein at least one of the two devices compares the values measured to the reference values, and wherein at least one of the two devices acts on the data exchange when the measured parameters differ from the reference values more than a threshold value.

26. (Previously Presented) Data exchange method according to claim 25, wherein at least one of the two devices acts by stopping the data exchange between the two devices.

27. (Previously Presented) Data exchange method according to claim 25, wherein the session key is regenerated in function of a determined parameter of use and wherein the determined parameter of use is the representative physical parameter of the communication.

28. (Previously Presented) Data exchange method according to claim 17, wherein

- at least one of the devices generates at least one supplementary random number,
- this supplementary random number is encrypted by said first encrypting key,
- this supplementary encrypted random number is transmitted to the second device,
- this transmitted encrypted supplementary random number is decrypted in this second device,
- the decrypted supplementary random number is encrypted by said second encrypting key,
- the supplementary encrypted random number is transmitted to the first device,
- the supplementary random number decrypted in the first device is compared to the initial supplementary random number generated in said first device,
- the information exchange is interrupted if the comparison indicates that the two compared numbers are not identical.

29. (Previously Presented) Data exchange method according to claim 17, wherein

- at least one of the devices determines at least one predefined fixed number memorized in the two devices,
- this predefined fixed number is encrypted by said first encrypting key,
- this predefined fixed encrypted number is transmitted to the second device,
- this transmitted encrypted predefined fixed number is decrypted in this second device,
- the predefined fixed number decrypted in the second device is compared to the predefined fixed number memorized in this second device,
- the data exchange is interrupted if the comparison indicates that the two compared numbers are not identical.

30. (Previously Presented) Data exchange method according to claim 28, wherein each of the numbers is encrypted separately.

31. (Previously Presented) Data exchange method according to claim 29, wherein each of the numbers is encrypted separately.

32. (Previously Presented) Data exchange method according to claim 28, wherein a combination of each of the numbers is encrypted.

33. (Previously Presented) Data exchange method according to claim 29, wherein a combination of each of the numbers is encrypted.

34. (Previously Presented) Receiver for carrying out the method according to claim 17, this receiver comprising at least one calculation unit, a read-only memory, a demultiplexer, a descrambler, a digital/analog converter, an external

memory and a sound and image descrambler, wherein at least the calculation unit, the read-only memory and the descrambler are contained in a same electronic chip and wherein at least one of the encrypting keys is stored in said electronic chip.

35. (Previously Presented) Receiver according to claim 34, wherein at least one of the numbers is stored in said electronic chip.

36. (New) A data exchange method between a security module locally connected to a receiver, the security module including a first encrypting key of a pair of asymmetric keys and the receiver including a second encrypting key of said pair of asymmetric keys, the method comprising:

generating, at least one first random number in the security module,

generating, at least one second random number in the receiver,

encrypting said first random number by said first encrypting key, the first encrypting key initialized in the security module during an initialization phase of the security module in a first protected environment,

encrypting said second random number by said second encrypting key, the second encrypting key initialized in the receiver during an initialization phase of the receiver in a second protected environment,

transmitting said encrypted first random number to the receiver,

transmitting said encrypted second random number to the security module,

decrypting the encrypted first random number in the receiver,

decrypting the encrypted second random number in the security module,

combining the decrypted second random number with the first random number generated in the security module, and combining the decrypted first random number with the second random number generated in the receiver, said combinations generating a session key in the security module and the receiver, and

using the session key to encrypt and decrypt at least a portion of data exchanged between the security module and receiver, wherein

the encrypted first random number, transmitted to the receiver and decrypted by the receiver, is

encrypted by the receiver using the second encrypting key,

transmitted in an encrypted form to the security module,

decrypted in the security module using the first encrypting key, and

compared with the first random number previously generated in the security module, and

a data transfer between the security module and the receiver is stopped if the compared random numbers are not identical.

--END CLAIM RECITATION--